(5)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179627
(43)Date of publication of application : 27.06.2003

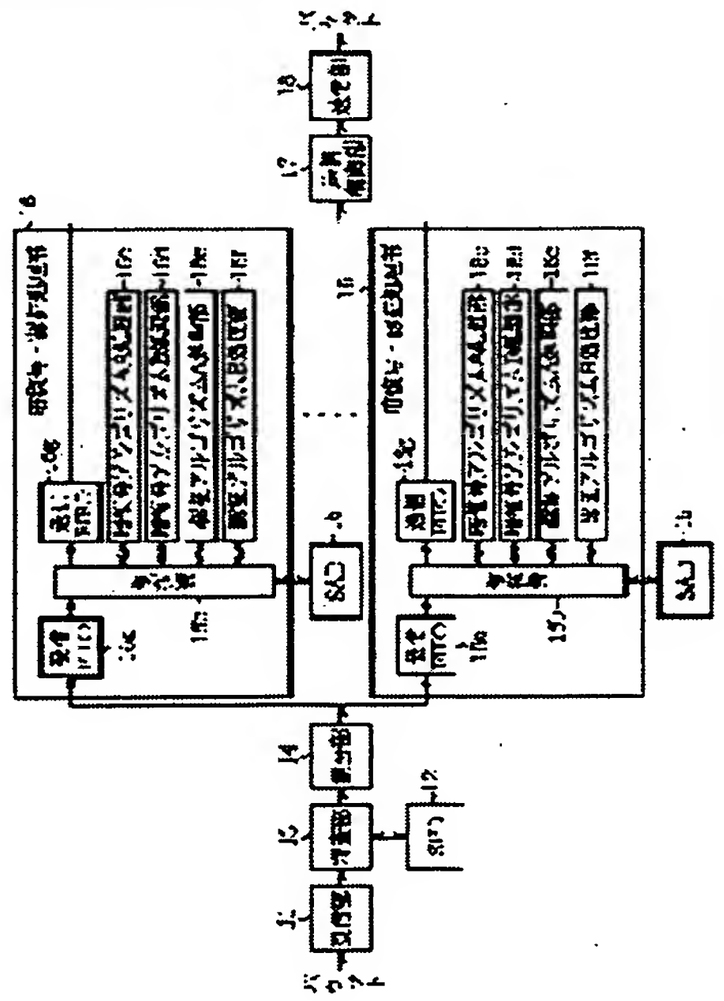
(51)Int.Cl. H04L 12/56
G09C 1/00
H04L 9/36
H04L 12/22

(21)Application number : 2001-376217
(22)Date of filing : 10.12.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KONUKI JUNJI

(54) PACKET COMMUNICATION EQUIPMENT AND PACKET COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide packet communication equipment capable of promptly starting execution of a cipher processing or the like, and a packet communication method.
SOLUTION: At the time of receiving a packet to which an index is added, a cipher algorithm and a key for ciphering, etc., are acquired from a specific entry specified by the index and the cipher processing or the like to the packet is executed.



LEGAL STATUS

[Date of request for examination] 15.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－179627
（P2003－179627A）
(43)公開日　平成15年６月27日(2003.6.27)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	12/56		Ｈ０４Ｌ 12/56	Ｚ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ 1/00	６６０Ｅ	５Ｋ０３０
Ｈ０４Ｌ	9/36		Ｈ０４Ｌ 12/22		
	12/22		9/00	６８５	

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－376217(P2001－376217)

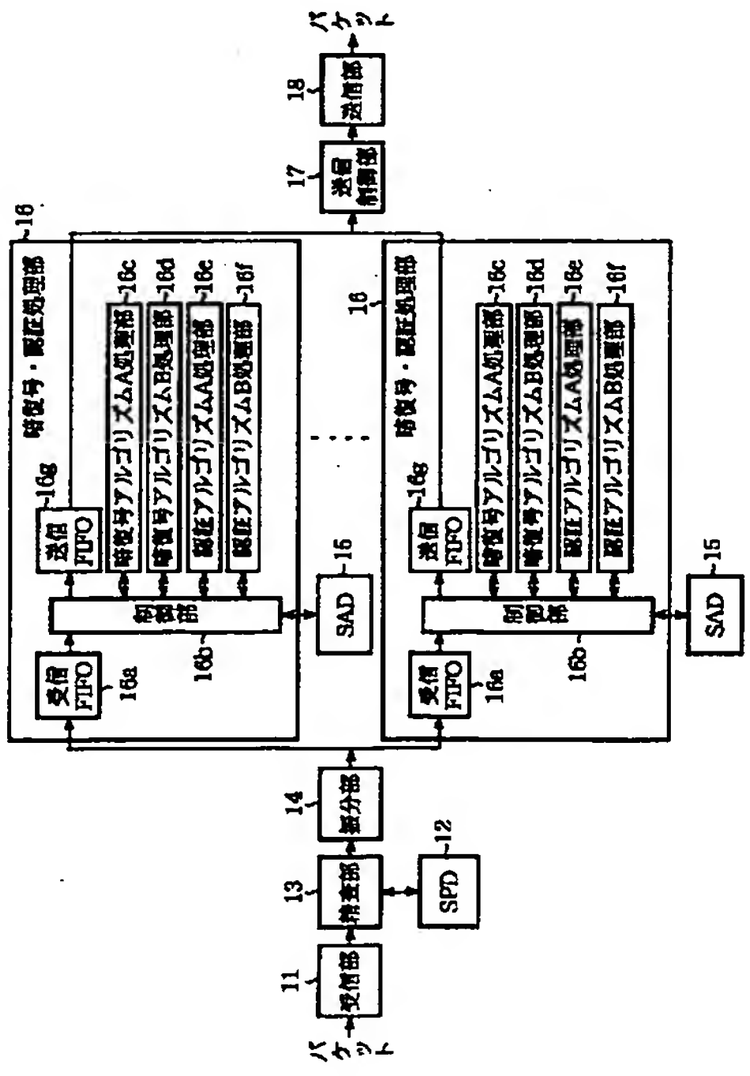
(22)出願日　平成13年12月10日(2001.12.10)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　小貫　淳史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100066474
弁理士　田澤　博昭　（外１名）

Ｆターム(参考)　5J104 AA18 DA04 EA16 JA31 NA01 PA07
5K030 GA15 HA08 JA05 KA07 LD19

(54)【発明の名称】　パケット通信装置及びパケット通信方法

(57)【要約】
【課題】　振分部５がパケットを暗復号・認証処理部６に転送する際、暗号アルゴリズムや暗号鍵等をパケットに付加して転送する必要がある。このため、パケットの通信路の帯域が圧迫されて、そのパケットの転送に長時間を要し、暗復号・認証処理部６が速やかに暗号処理や認証処理の実行を開始することができない課題があった。
【解決手段】　インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、そのパケットに対する暗号処理等を実行する。



【特許請求の範囲】

【請求項１】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのパケットに対する暗号処理を実行する処理実行手段とを備えたパケット通信装置。

【請求項２】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を実行する処理実行手段とを備えたパケット通信装置。

【請求項３】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行する処理実行手段とを備えたパケット通信装置。

【請求項４】　複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してパケットを出力することを特徴とする請求項１から請求項３のうちのいずれか１項記載のパケット通信装置。

【請求項５】　各処理実行手段毎に同一のデータベースを設けたことを特徴とする請求項４記載のパケット通信装置。

【請求項６】　データベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットに格納されているデータにしたがって上記データベースを更新する更新手段を設けたことを特徴とする請求項１から請求項５のうちのいずれか１項記載のパケット通信装置。

【請求項７】　インデックス付加手段は、データベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットをバッファに一時的に保存し、処理実行手段は未処理のパケットが存在しないとき当該特定パケットを取得し、その特定パケットに格納されているデータにしたがって上記データベースを更新することを特徴とする請求項１から請求項５のうちのいずれか１項記載のパケット通信装置。

【請求項８】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加して出力する一方、そのインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのパケットに対する暗号処理を実行するパケット通信方法。

【請求項９】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加して出力する一方、そのインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を実行するパケット通信方法。

【請求項１０】　パケットを受信すると、そのパケットに係るデータベース内の特定エントリを指定するインデックスを当該パケットに付加して出力する一方、そのインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行するパケット通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、パケットに対する暗号処理や認証処理を行うパケット通信装置及びパケット通信方法に関するものである。

【０００２】

【従来の技術】近年のインターネットの普及に伴って、それらを利用した企業間のデータ通信が増えてきている。そのためデータの盗聴や改竄が大きな問題となっている。この問題を解決するには、暗号技術と認証技術が必須となる。通信装置間を接続する通信路上を流れるパケットを暗号化し、さらに認証コードを付加して送受信することにより、パケットの盗聴および改竄を防止することができる。

【０００３】特に、最近では、処理するパケットの宛先アドレスやプロトコルに応じて暗号のアルゴリズムや認証のアルゴリズムを変更できる場合が多い。ここでは、そのような通信装置を考える。また、暗号処理や認証処理には膨大な計算量が必要であり、そのため通信装置内に暗号処理や認証処理を実行するパケット処理系を複数配置して、それらの間で並列処理を行う方式を用いる場合が多い。

【０００４】図７は従来のパケット通信装置を示す構成図であり、図において、１は外部装置からパケットを受信する受信部、２は各パケットの宛先アドレスやセキュリティアソシエーションデータベース（以下、ＳＡＤという）４内の特定エントリを指定するインデックス等を格納するセキュリティポリシーデータベース（以下、ＳＰＤという）、３は受信部１により受信されたパケットからＩＰヘッダを取り出し、そのＩＰヘッダ内の宛先アドレスをキーにして、ＳＰＤ２から当該パケットに係るＳＡＤ４内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得する精査

部である。

【０００５】４はパケットに対する暗号アルゴリズムや暗号用鍵等から構成されるエントリを複数個格納するＳＡＤ、５は精査部３により取得されたインデックスが指定するＳＡＤ４内の特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、これらの暗号アルゴリズム等を当該パケットに付加し、そのパケットを未処理中の暗復号・認証処理部６に転送する振分部、６は振分部５により転送されたパケットから暗号アルゴリズム等を取り出して、そのパケットに対する暗号処理や認証処理を実行する暗復号・認証処理部、７は各暗復号・認証処理部６による処理後のパケットの順序を整列して、受信部１により受信されたパケットの順序に合わせる送信制御部、８は送信制御部７から出力されたパケットを送信する送信部である。

【０００６】次に動作について説明する。受信部１が例えば平文データが格納されているパケットを受信すると、精査部３は、受信部１により受信されたパケットからＩＰヘッダを取り出し、そのＩＰヘッダからパケットの宛先アドレスを取得する。そして、精査部３は、その宛先アドレスをキーにして、ＳＰＤ２から当該パケットに係るＳＡＤ４内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得する。

【０００７】振分部５は、精査部３がＳＡＤ４内の特定エントリを指定するインデックスを取得すると、そのインデックスが指定するＳＡＤ４内の特定エントリから暗号アルゴリズム、認証アルゴリズム、暗号用鍵及び認証用鍵を取得する。そして、振分部５は、特定エントリから取得した暗号アルゴリズム等を当該パケットに付加し、そのパケットを未処理中の暗復号・認証処理部６に転送する。

【０００８】暗復号・認証処理部６は、振分部５からパケットを受けると、そのパケットから暗号アルゴリズム等を取り出し、そのパケットに対する暗号処理や認証処理を実行する。送信制御部７は、各暗復号・認証処理部６から処理後のパケットを受けると、処理後のパケットの順序を整列して、受信部１により受信されたパケットの順序に合わせるようにする。送信部８は、送信制御部７から出力されたパケットを外部装置に送信する。

【０００９】

【発明が解決しようとする課題】従来のパケット通信装置は以上のように構成されているので、振分部５がパケットを暗復号・認証処理部６に転送する際、暗号アルゴリズムや暗号鍵等をパケットに付加して転送する必要がある。このため、パケットの通信路の帯域が圧迫されて、そのパケットの転送に長時間を要し、暗復号・認証処理部６が速やかに暗号処理や認証処理の実行を開始することができない課題があった。

【００１０】この発明は上記のような課題を解決するためになされたもので、速やかに暗号処理等の実行を開始することができるパケット通信装置及びパケット通信方法を得ることを目的とする。

【００１１】

【課題を解決するための手段】この発明に係るパケット通信装置は、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのパケットに対する暗号処理を実行する処理実行手段を設けたものである。

【００１２】この発明に係るパケット通信装置は、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を実行する処理実行手段を設けたものである。

【００１３】この発明に係るパケット通信装置は、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行する処理実行手段を設けたものである。

【００１４】この発明に係るパケット通信装置は、複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してパケットを出力するようにしたものである。

【００１５】この発明に係るパケット通信装置は、各処理実行手段毎に同一のデータベースを設けたものである。

【００１６】この発明に係るパケット通信装置は、データベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットに格納されているデータにしたがってデータベースを更新する更新手段を設けたものである。

【００１７】この発明に係るパケット通信装置は、インデックス付加手段がデータベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットをバッファに一時的に保存し、処理実行手段が未処理のパケットが存在しないとき特定パケットを取得し、その特定パケットに格納されているデータにしたがってデータベースを更新するようにしたものである。

【００１８】この発明に係るパケット通信方法は、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのパケットに対する暗号処理を実行するようにしたものである。

【００１９】この発明に係るパケット通信方法は、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を

実行するようにしたものである。

【００２０】この発明に係るパケット通信方法は、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行するようにしたものである。

【００２１】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．図１はこの発明の実施の形態１によるパケット通信装置を示す構成図であり、図において、１１は外部装置からパケットを受信する受信部、１２は各パケットの送信先アドレスやＳＡＤ１５内の特定エントリを指定するインデックス等を格納するＳＰＤ、１３は受信部１１により受信されたパケットからＩＰヘッダを取り出し、そのＩＰヘッダ内の送信先アドレス等をキーにして、ＳＰＤ１２から当該パケットに係るＳＡＤ１５内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得し、そのインデックスを当該パケットに付加する精査部、１４は精査部１３によりインデックスが付加されたパケットを未処理中の暗復号・認証処理部１６に転送する振分部である。なお、受信部１１，ＳＰＤ１２，精査部１３及び振分部１４からインデックス付加手段が構成されている。

【００２２】１５はパケットに対する暗号アルゴリズムや暗号用鍵等から構成されるエントリを複数個格納するＳＡＤ（データベース）、１６は振分部１４からパケットを受けると、そのパケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取り出して、そのパケットに対する暗号処理や認証処理を実行する暗復号・認証処理部（処理実行手段）、１６ａは振分部１４から転送されたパケットを受信して格納する受信ＦＩＦＯ、１６ｂは受信ＦＩＦＯ１６ａに格納されているパケットを取得して、そのパケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取り出し、各種処理部を制御する制御部、１６ｃは暗号アルゴリズムＡを実行する暗復号アルゴリズムＡ処理部、１６ｄは暗号アルゴリズムＢを実行する暗復号アルゴリズムＢ処理部、１６ｅは認証アルゴリズムＡを実行する認証アルゴリズムＡ処理部、１６ｆは認証アルゴリズムＢを実行する認証アルゴリズムＢ処理部、１６ｇは処理後のパケットを格納する送信ＦＩＦＯである。

【００２３】１７は各暗復号・認証処理部１６による処理後のパケットの順序を整列して、受信部１１により受信されたパケットの順序に合わせる送信制御部、１８は送信制御部１７から出力されたパケットを送信する送信部である。なお、図３及び図４はこの発明の実施の形態１によるパケット通信方法を示すフローチャートである。

【００２４】次に動作について説明する。最初に平文データが格納されているパケットを暗号化して、そのパケットに認証コード（認証用のダイジェスト）を付加する場合について説明する。受信部１１が外部装置から平文データが格納されているパケットを受信すると、そのパケットのＭＡＣヘッダを削除して精査部１３に出力する（ステップＳＴ１）。

【００２５】精査部１３は、受信部１１からパケットを受けると、そのパケットからＩＰヘッダを取り出し、そのＩＰヘッダからパケットの送信元アドレス、送信先アドレスやプロトコル等を取得する。そして、精査部１３は、そのアドレスやプロトコルと一致するＳＰＤ１２内のエントリを検索する（ステップＳＴ２）。

【００２６】即ち、ＳＰＤ１２は、図２に示すように、送信元アドレス、送信先アドレス、プロトコル、送信先ポート番号、送信元ポート番号、ＳＰＩ、処理指定（パケットに対する処理内容）、及びインデックス（ＳＡＤ１５内の特定エントリのアドレスを示すポインタ）から構成された複数個のエントリを格納しているので、ＩＰヘッダから取得したアドレスやプロトコルと一致する内容を有するエントリを検索する。ただし、必要に応じて送信先アドレスのみが一致するエントリを検索するようにしてもよいし、送信元アドレスと送信先アドレスとプロトコルとが一致するエントリを検索するようにしてもよい。

【００２７】精査部１３は、上記のようにしてＳＰＤ１２内のエントリを検索すると、そのエントリ内のインデックスを当該パケットに付加して振分部１４に出力する（ステップＳＴ３）。ただし、そのエントリ内の処理指定が“暗号・認証”ではなく、“棄却”である場合には、そのパケットを出力せずに廃棄する。振分部１４は、精査部１３からインデックスが付加されたパケットを受けると、受信ＦＩＦＯ１６ａが空き状態の暗復号・認証処理部１６を一つ選択し、その暗復号・認証処理部１６に対して当該パケットを転送する（ステップＳＴ４）。なお、インデックスは、暗号アルゴリズムや暗号用鍵等と比べて、極めて少ない情報量であるため、パケットの通信路の帯域を圧迫するようなことはない。

【００２８】暗復号・認証処理部１６の制御部１６ｂは、受信ＦＩＦＯ１６ａが振分部１４から転送されたパケットを受信して格納すると、受信ＦＩＦＯ１６ａからパケットを取得し、図２に示すように、そのパケットに付加されているインデックスが指定するＳＡＤ１５内の特定エントリから暗号アルゴリズムや暗号用鍵等を取得する（ステップＳＴ５）。

【００２９】即ち、ＳＡＤ１５は、図２に示すように、暗号アルゴリズム、認証アルゴリズム、暗号用鍵及び認証用鍵等から構成された複数個のエントリを格納しているので、そのパケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵

等を取得する。なお、ＳＡＤ１５は、通常、ＳＲＡＭやＤＲＡＭなどのメモリにより実現される。

【００３０】そして、暗復号・認証処理部１６の制御部１６ｂは、特定エントリから取得した暗号アルゴリズムが例えば暗号アルゴリズムＡであれば、暗復号アルゴリズムＡ処理部１６ｃを起動し、例えば暗号アルゴリズムＢであれば、暗復号アルゴリズムＢ処理部１６ｄを起動する。暗復号アルゴリズムＡ処理部１６ｃ又は暗復号アルゴリズムＢ処理部１６ｄは、制御部１６ｂから起動指令を受けると、制御部１６ｂから出力された暗号用鍵を用いて暗号アルゴリズムＡ又は暗号アルゴリズムＢを実行することにより、そのパケット内の暗号処理の対象ブロックを暗号化する（ステップＳＴ６）。

【００３１】暗復号・認証処理部１６の制御部１６ｂは、暗復号アルゴリズムＡ処理部１６ｃ又は暗復号アルゴリズムＢ処理部１６ｄの暗号化処理が完了すると、特定エントリから取得した認証アルゴリズムが例えば認証アルゴリズムＡであれば、認証アルゴリズムＡ処理部１６ｅを起動し、例えば認証アルゴリズムＢであれば、認証アルゴリズムＢ処理部１６ｆを起動する。認証アルゴリズムＡ処理部１６ｅ又は認証アルゴリズムＢ処理部１６ｆは、制御部１６ｂから起動指令を受けると、制御部１６ｂから出力された認証用鍵を用いて認証アルゴリズムＡ又は認証アルゴリズムＢを実行することにより、認証用のダイジェストを生成する（ステップＳＴ７）。

【００３２】暗復号・認証処理部１６の制御部１６ｂは、認証アルゴリズムＡ処理部１６ｅ又は認証アルゴリズムＢ処理部１６ｆが認証用のダイジェストを生成すると、暗復号アルゴリズムＡ処理部１６ｃ又は暗復号アルゴリズムＢ処理部１６ｄにより暗号化されたパケットに当該ダイジェストを付加し、ＩＰヘッダを生成してパケットのエンカプセル処理を行う（ステップＳＴ８）。そして、エンカプセル処理が完了すると、処理後のパケットを送信ＦＩＦＯ１６ｇに格納する。

【００３３】送信制御部１７は、各暗復号・認証処理部１６の送信ＦＩＦＯ１６ｇから処理後のパケットを取り出して、処理後のパケットの順序を整列し、受信部１１により受信されたパケットの順序に合わせるようにする（ステップＳＴ９）。送信部１８は、送信制御部１７から出力されたパケットにＭＡＣヘッダを付加して外部装置に送信する（ステップＳＴ１０）。

【００３４】次に暗号文データが格納されているパケットに対する認証処理を実施して、そのパケットを復号化する場合について説明する。受信部１１が外部装置から暗号文データが格納されているパケットを受信すると、そのパケットのＭＡＣヘッダを削除して精査部１３に出力する（ステップＳＴ１１）。

【００３５】精査部１３は、受信部１１からパケットを受けると、そのパケットからＩＰヘッダを取り出し、そのＩＰヘッダからパケットの送信元アドレス、送信先アドレスやプロトコル等を取得する。そして、精査部１３は、そのアドレスやプロトコルと一致するＳＰＤ１２内のエントリを検索する（ステップＳＴ１２）。

【００３６】即ち、ＳＰＤ１２は、図２に示すように、送信元アドレス、送信先アドレス、プロトコル、送信先ポート番号、送信元ポート番号、ＳＰＩ、処理指定（パケットに対する処理内容）、及びインデックス（ＳＡＤ１５内の特定エントリのアドレスを示すポインタ）から構成された複数個のエントリを格納しているので、ＩＰヘッダから取得したアドレスやプロトコルと一致する内容を有するエントリを検索する。ただし、必要に応じて送信先アドレスのみが一致するエントリを検索するようにしてもよいし、送信元アドレスと送信先アドレスとプロトコルとが一致するエントリを検索するようにしてもよい。

【００３７】精査部１３は、上記のようにしてＳＰＤ１２内のエントリを検索すると、そのエントリ内のインデックスを当該パケットに付加して振分部１４に出力する（ステップＳＴ１３）。ただし、そのエントリ内の処理指定が“復号・認証”ではなく、“棄却”である場合には、そのパケットを出力せずに廃棄する。振分部１４は、精査部１３からインデックスが付加されたパケットを受けると、受信ＦＩＦＯ１６ａが空き状態の暗復号・認証処理部１６を一つ選択して、その暗復号・認証処理部１６に対して当該パケットを転送する（ステップＳＴ１４）。なお、インデックスは、復号アルゴリズムや認証用鍵等と比べて、極めて少ない情報量であり、パケットの通信路の帯域を圧迫するようなことはない。

【００３８】暗復号・認証処理部１６の制御部１６ｂは、受信ＦＩＦＯ１６ａが振分部１４から転送されたパケットを受信して格納すると、受信ＦＩＦＯ１６ａからパケットを取得し、図２に示すように、そのパケットに付加されているインデックスが指定するＳＡＤ１５内の特定エントリから復号アルゴリズムや認証用鍵等を取得する（ステップＳＴ１５）。

【００３９】即ち、ＳＡＤ１５は、図２に示すように、復号アルゴリズム、認証アルゴリズム、復号用鍵及び認証用鍵等から構成された複数個のエントリを格納しているので、そのパケットに付加されているインデックスが指定する特定エントリから復号アルゴリズムや復号用鍵等を取得する。

【００４０】そして、暗復号・認証処理部１６の制御部１６ｂは、特定エントリから取得した認証アルゴリズムが例えば認証アルゴリズムＡであれば、認証アルゴリズムＡ処理部１６ｅを起動し、例えば認証アルゴリズムＢであれば、認証アルゴリズムＢ処理部１６ｆを起動する。認証アルゴリズムＡ処理部１６ｅ又は認証アルゴリズムＢ処理部１６ｆは、制御部１６ｂから起動指令を受けると、制御部１６ｂから出力された認証用鍵を用いて認証アルゴリズムＡ又は認証アルゴリズムＢを実行する

ことにより、認証用のダイジェストを生成する（ステップＳＴ１６）。

【００４１】暗復号・認証処理部１６の制御部１６ｂは、認証アルゴリズムＡ処理部１６ｅ又は認証アルゴリズムＢ処理部１６ｆが認証用のダイジェストを生成すると、そのダイジェストと、受信ＦＩＦＯ１６ａから取得したパケットに付加されているダイジェストとを比較する（ステップＳＴ１７）。両者が一致する場合には、認証の成功を認定し、両者が一致しない場合には、認証の失敗を認定して、そのパケットを廃棄する（ステップＳＴ１８）。

【００４２】暗復号・認証処理部１６の制御部１６ｂは、上記のようにして認証の成功を認定すると、特定エントリから取得した復号アルゴリズムが例えば復号アルゴリズムＡであれば、暗復号アルゴリズムＡ処理部１６ｃを起動し、例えば復号アルゴリズムＢであれば、暗復号アルゴリズムＢ処理部１６ｄを起動する。暗復号アルゴリズムＡ処理部１６ｃ又は暗復号アルゴリズムＢ処理部１６ｄは、制御部１６ｂから起動指令を受けると、制御部１６ｂから出力された復号用鍵を用いて復号アルゴリズムＡ又は復号アルゴリズムＢを実行することにより、そのパケット内の復号処理の対象ブロックを復号化する（ステップＳＴ１９）。

【００４３】暗復号・認証処理部１６の制御部１６ｂは、暗復号アルゴリズムＡ処理部１６ｃ又は暗復号アルゴリズムＢ処理部１６ｄの復号化処理が完了すると、復号化されたパケットからＩＰヘッダを削除して、パケットのデカプセル処理を行う。そして、デカプセル処理が完了すると、処理後のパケットを送信ＦＩＦＯ１６ｇに格納する。

【００４４】送信制御部１７は、各暗復号・認証処理部１６の送信ＦＩＦＯ１６ｇから処理後のパケットを取り出して、処理後のパケットの順序を整列し、受信部１１により受信されたパケットの順序に合わせるようにする（ステップＳＴ２０）。送信部１８は、送信制御部１７から出力されたパケットにＭＡＣヘッダを付加して外部装置に送信する（ステップＳＴ２１）。

【００４５】以上で明らかなように、この実施の形態１によれば、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、そのパケットに対する暗号処理等を実行するように構成したので、パケット通信路の帯域圧迫を招くことなく、暗号処理や認証処理等を実行することができる結果、速やかに暗号処理や認証処理の実行を開始することができる効果を奏する。また、この実施の形態１によれば、各暗復号・認証処理部１６毎に同一のＳＡＤ１５を設けるように構成したので、並列化された各暗復号・認証処理部１６は、他の暗復号・認証処理部１６がＳＡＤ１５にアクセスしているときも、そのアクセスの完了を待つことなく、ＳＡＤ１５にアクセスすることができる結果、速やかに暗号処理や認証処理の実行を開始することができる効果を奏する。

【００４６】実施の形態２．図５はこの発明の実施の形態２によるパケット通信装置を示す構成図であり、図において、図１と同一符号は同一または相当部分を示すので説明を省略する。１９はＳＡＤ１５に格納されている情報を変更するための特定パケットを受信すると、その特定パケットに格納されているデータにしたがってＳＡＤ１５を更新するＳＡＤ更新部（更新手段）である。

【００４７】次に動作について説明する。上記実施の形態１では、ＳＡＤ１５に格納されているエントリ内の情報変更については特に言及していないが、ＳＡＤ１５に格納されているエントリ内の情報を変更するようにしてもよい。

【００４８】即ち、受信部１１がＳＡＤ１５に格納されている情報を変更するための特定パケットを受信すると、振分部１４が当該特定パケットをＳＡＤ更新部１９に出力する。ＳＡＤ更新部１９は、振分部１４から特定パケットを受けると、その特定パケットに格納されているデータにしたがってＳＡＤ１５に格納されているエントリ内の情報を変更する。なお、ＳＡＤ１５に対するエントリの追加や削除を行うようにしてもよい。

【００４９】実施の形態３．上記実施の形態２では、ＳＡＤ更新部１９が特定パケットに格納されているデータにしたがってＳＡＤ１５に格納されているエントリ内の情報を変更するものについて示したが、図６に示すように、ＳＡＤ更新部１９の代わりに、一時保存バッファ２０を設けることにより、ＳＡＤ１５を更新するようにしてもよい。

【００５０】具体的には、受信部１１がＳＡＤ１５に格納されている情報を変更するための特定パケットを受信すると、精査部１３が通常のパケットを有している場合、通常のパケットの処理を優先するため、振分部１４が当該特定パケットを一時保存バッファ２０に待避する。

【００５１】振分部１４は、精査部１３において通常のパケットが無くなると、一時保存バッファ２０に保存されている特定パケットを各暗復号・認証処理部１６に転送する。各暗復号・認証処理部１６の制御部１６ｂは、精査部１３から特定パケットを受けると、その特定パケットに格納されているデータにしたがってＳＡＤ１５に格納されているエントリ内の情報を変更する。なお、ＳＡＤ１５に対するエントリの追加や削除を行うようにしてもよい。

【００５２】

【発明の効果】以上のように、この発明によれば、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、その

パケットに対する暗号処理を実行する処理実行手段を設けるように構成したので、速やかに暗号処理の実行を開始することができる効果がある。

【００５３】この発明によれば、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を実行する処理実行手段を設けるように構成したので、速やかに復号処理の実行を開始することができる効果がある。

【００５４】この発明によれば、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行する処理実行手段を設けるように構成したので、速やかに認証処理の実行を開始することができる効果がある。

【００５５】この発明によれば、複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してパケットを出力するように構成したので、処理の効率化を図ることができる効果がある。

【００５６】この発明によれば、各処理実行手段毎に同一のデータベースを設けるように構成したので、ある処理実行手段がデータベースにアクセスしているときも、そのアクセスの完了を待つことなく、その他の処理実行手段がデータベースにアクセスすることができる結果、速やかに暗号処理等の実行を開始することができる効果がある。

【００５７】この発明によれば、データベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットに格納されているデータにしたがってデータベースを更新する更新手段を設けるように構成したので、通常のパケットに対する処理に影響を与えることなく、データベースを更新することができる効果がある。

【００５８】この発明によれば、インデックス付加手段がデータベースに格納されている情報を変更するための特定パケットを受信すると、その特定パケットをバッファに一時的に保存し、処理実行手段が未処理のパケットが存在しないとき特定パケットを取得し、その特定パケットに格納されているデータにしたがってデータベースを更新するように構成したので、通常のパケットに対する処理に影響を与えることなく、データベースを更新することができる効果がある。

【００５９】この発明によれば、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのパケットに対する暗号処理を実行するように構成したので、速やかに暗号処理の実行を開始することができる効果がある。

【００６０】この発明によれば、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのパケットに対する復号処理を実行するように構成したので、速やかに復号処理の実行を開始することができる効果がある。

【００６１】この発明によれば、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのパケットに対する認証処理を実行するように構成したので、速やかに認証処理の実行を開始することができる効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１によるパケット通信装置を示す構成図である。

【図２】　ＳＰＤ及びＳＡＤの格納内容を示す説明図である。

【図３】　この発明の実施の形態１によるパケット通信方法を示すフローチャートである。

【図４】　この発明の実施の形態１によるパケット通信方法を示すフローチャートである。

【図５】　この発明の実施の形態２によるパケット通信装置を示す構成図である。

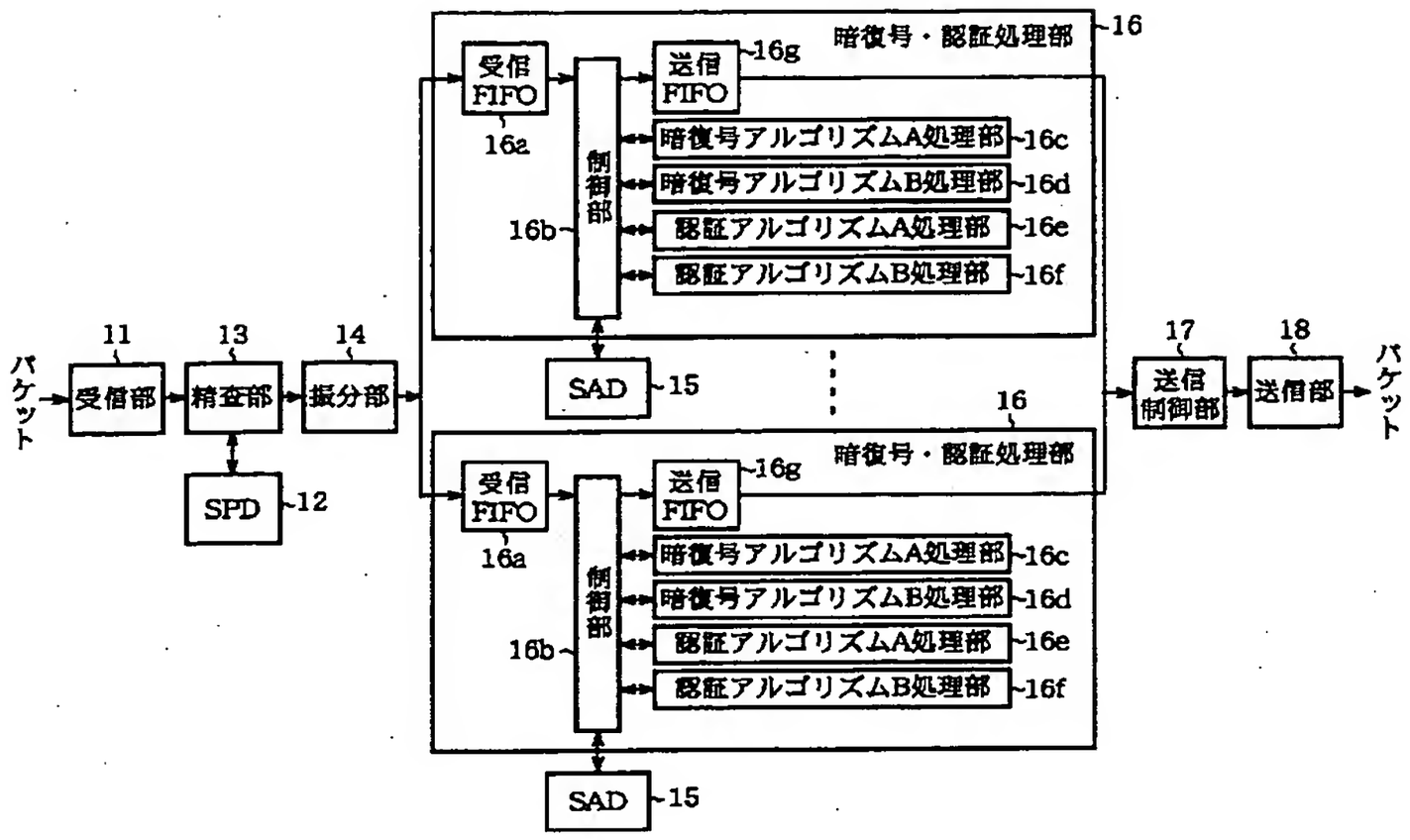
【図６】　この発明の実施の形態３によるパケット通信装置を示す構成図である。

【図７】　従来のパケット通信装置を示す構成図である。

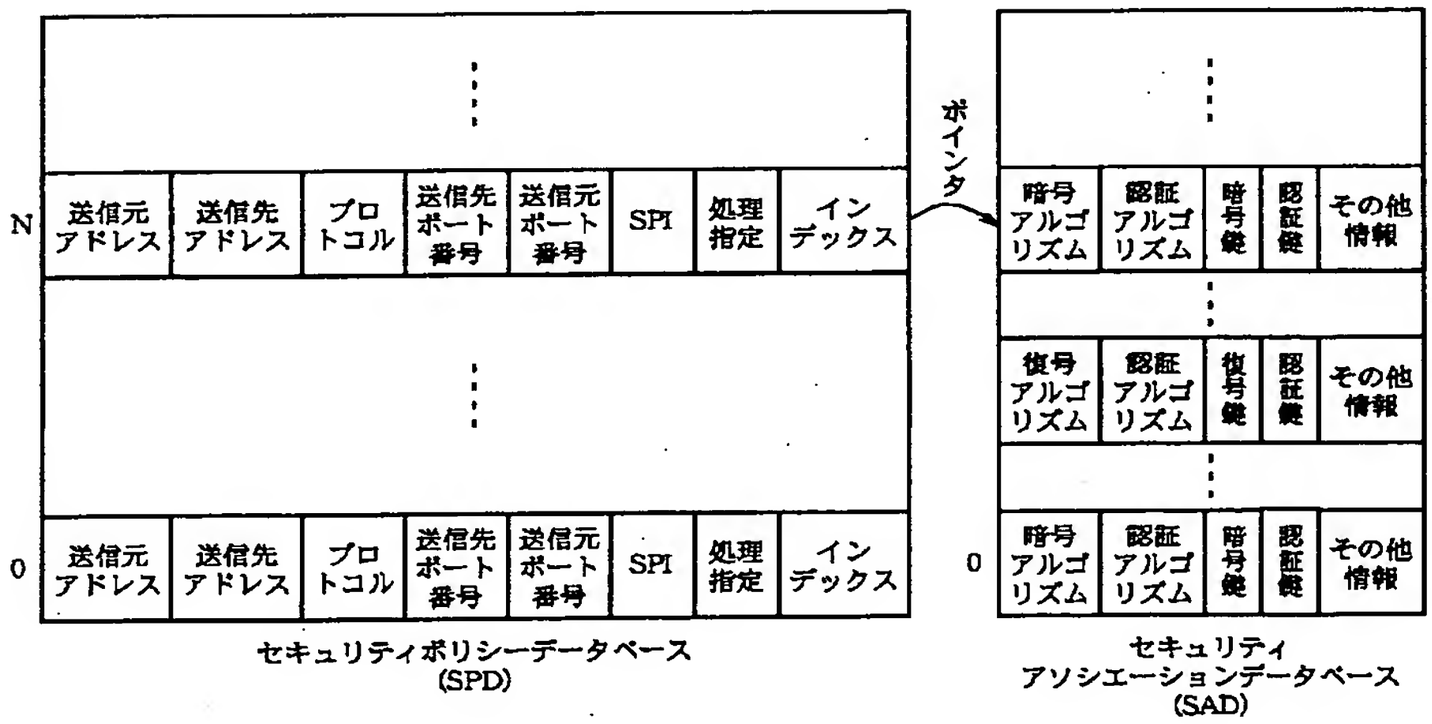
【符号の説明】

１１　受信部（インデックス付加手段）、１２　ＳＰＤ（インデックス付加手段）、１３　精査部（インデックス付加手段）、１４　振分部（インデックス付加手段）、１５　ＳＡＤ（データベース）、１６　暗復号・認証処理部（処理実行手段）、１６ａ　受信ＦＩＦＯ、１６ｂ　制御部、１６ｃ　暗復号アルゴリズムＡ処理部、１６ｄ　暗復号アルゴリズムＢ処理部、１６ｅ　認証アルゴリズムＡ処理部、１６ｆ　認証アルゴリズムＢ処理部、１６ｇ　送信ＦＩＦＯ、１７送信制御部、１８　送信部。

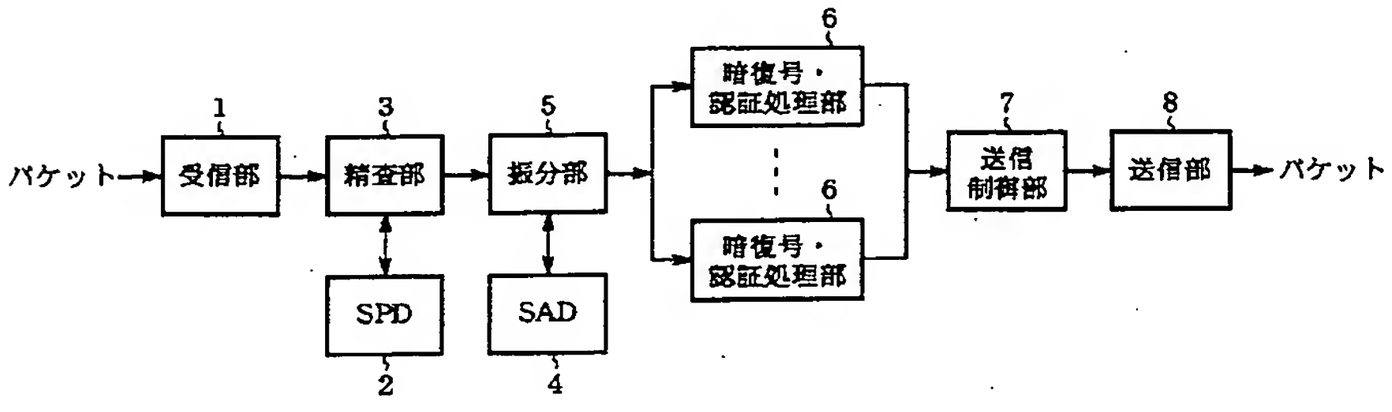
【図１】


パケット
11
受信部
13
精査部
14
振分部
SPD
12
SAD
15
暗復号・認証処理部
16
受信FIFO
16a
制御部
16b
送信FIFO
16g
暗復号アルゴリズムA処理部
16c
暗復号アルゴリズムB処理部
16d
認証アルゴリズムA処理部
16e
認証アルゴリズムB処理部
16f
17
送信制御部
18
送信部
パケット

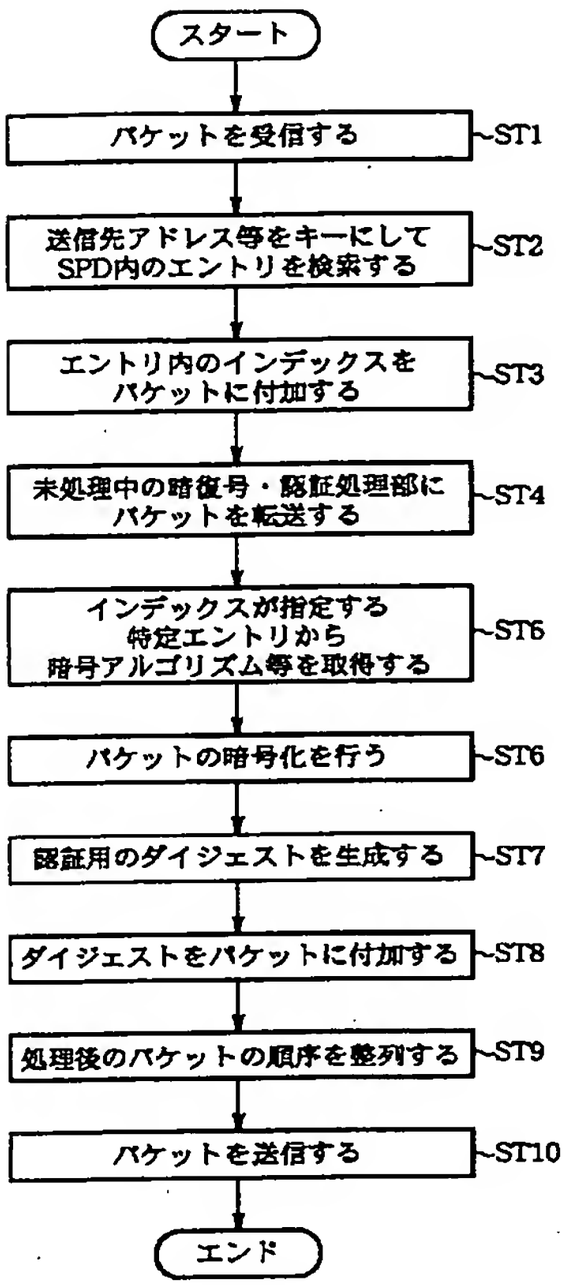
【図２】


N
0
送信元アドレス
送信先アドレス
プロトコル
送信先ポート番号
送信元ポート番号
SPI
処理指定
インデックス
ポインタ
暗号アルゴリズム
認証アルゴリズム
暗号鍵
認証鍵
その他情報
復号アルゴリズム
復号鍵
セキュリティポリシーデータベース
(SPD)
セキュリティ
アソシエーションデータベース
(SAD)

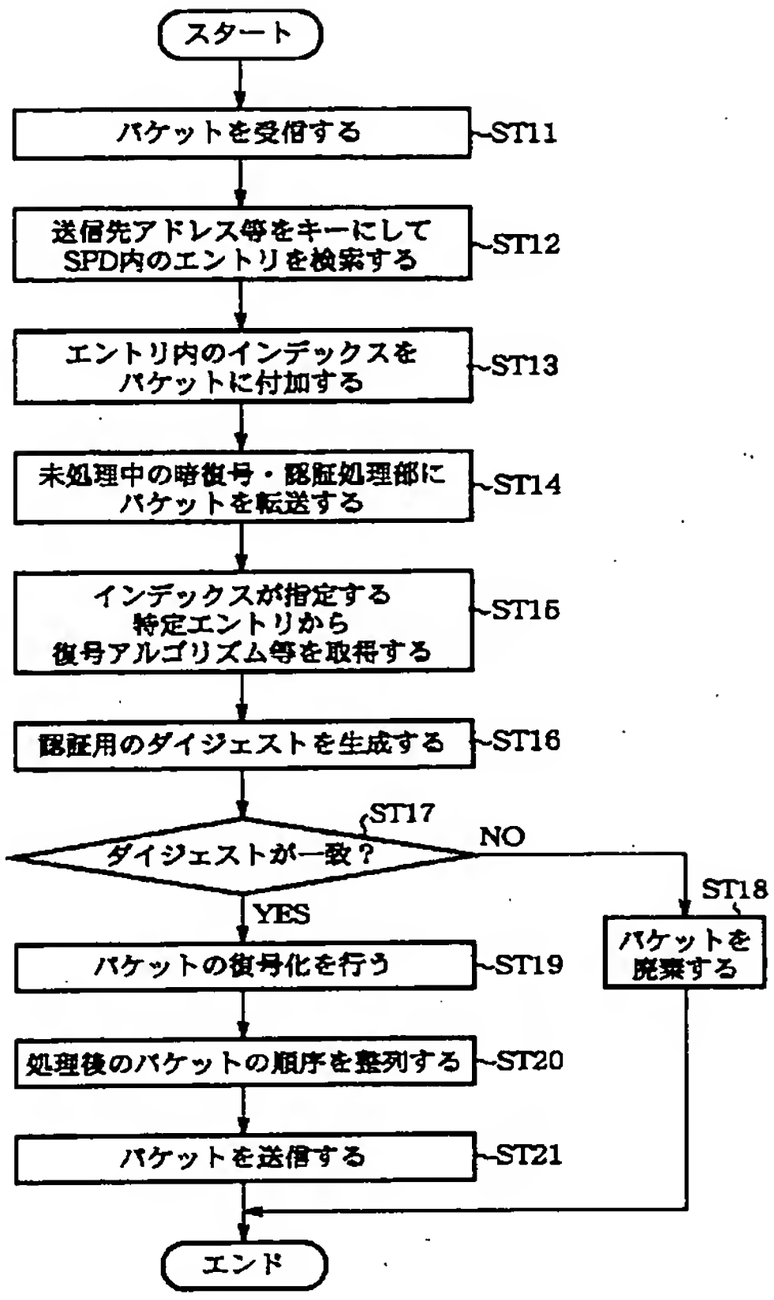
【図７】


パケット
1
受信部
3
精査部
5
振分部
6
暗復号・認証処理部
6
暗復号・認証処理部
7
送信制御部
8
送信部
パケット
SPD
2
SAD
4

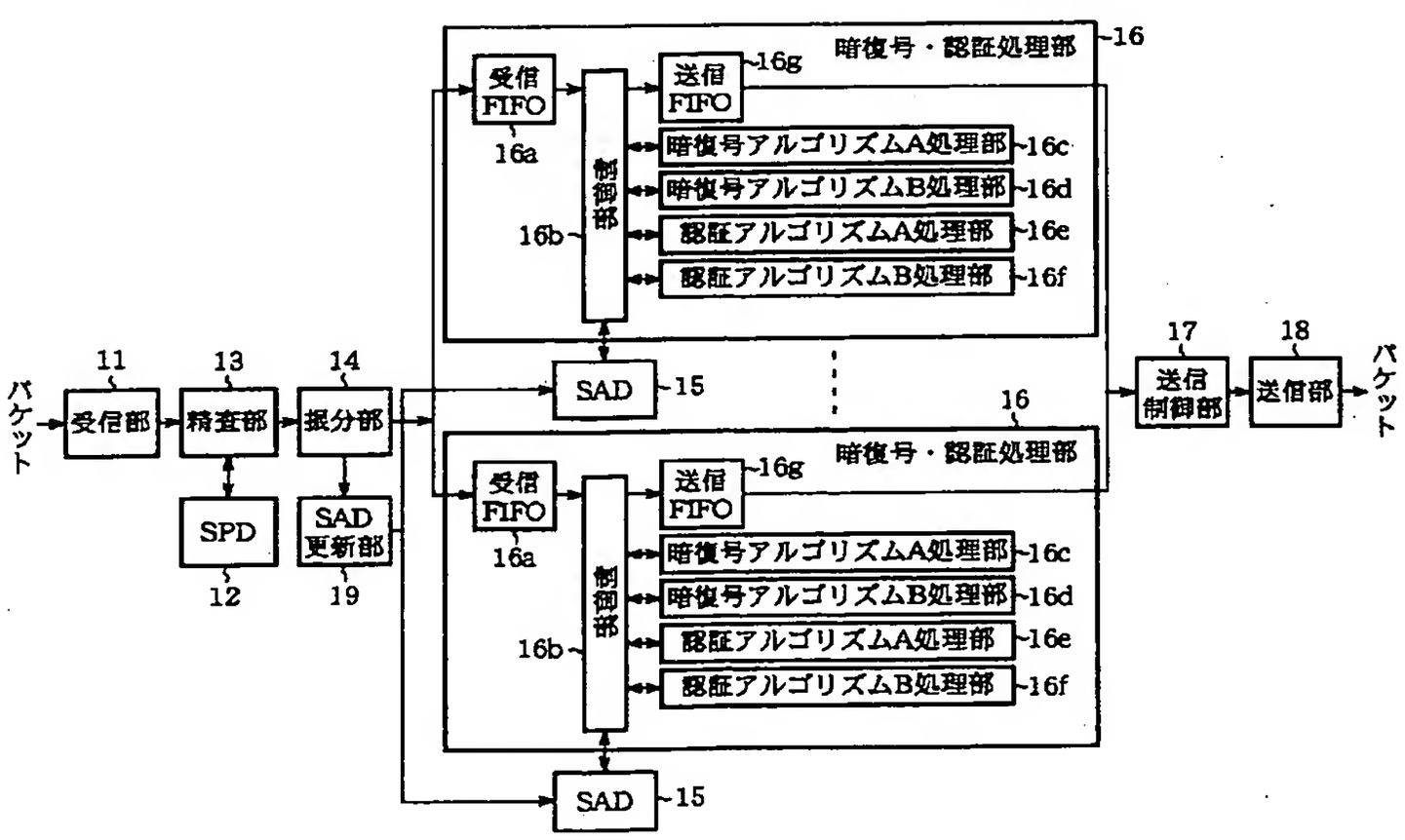
【図３】


スタート
パケットを受信する
ST1
送信先アドレス等をキーにして
SPD内のエントリを検索する
ST2
エントリ内のインデックスを
パケットに付加する
ST3
未処理中の暗復号・認証処理部に
パケットを転送する
ST4
インデックスが指定する
特定エントリから
暗号アルゴリズム等を取得する
ST5
パケットの暗号化を行う
ST6
認証用のダイジェストを生成する
ST7
ダイジェストをパケットに付加する
ST8
処理後のパケットの順序を整列する
ST9
パケットを送信する
ST10
エンド

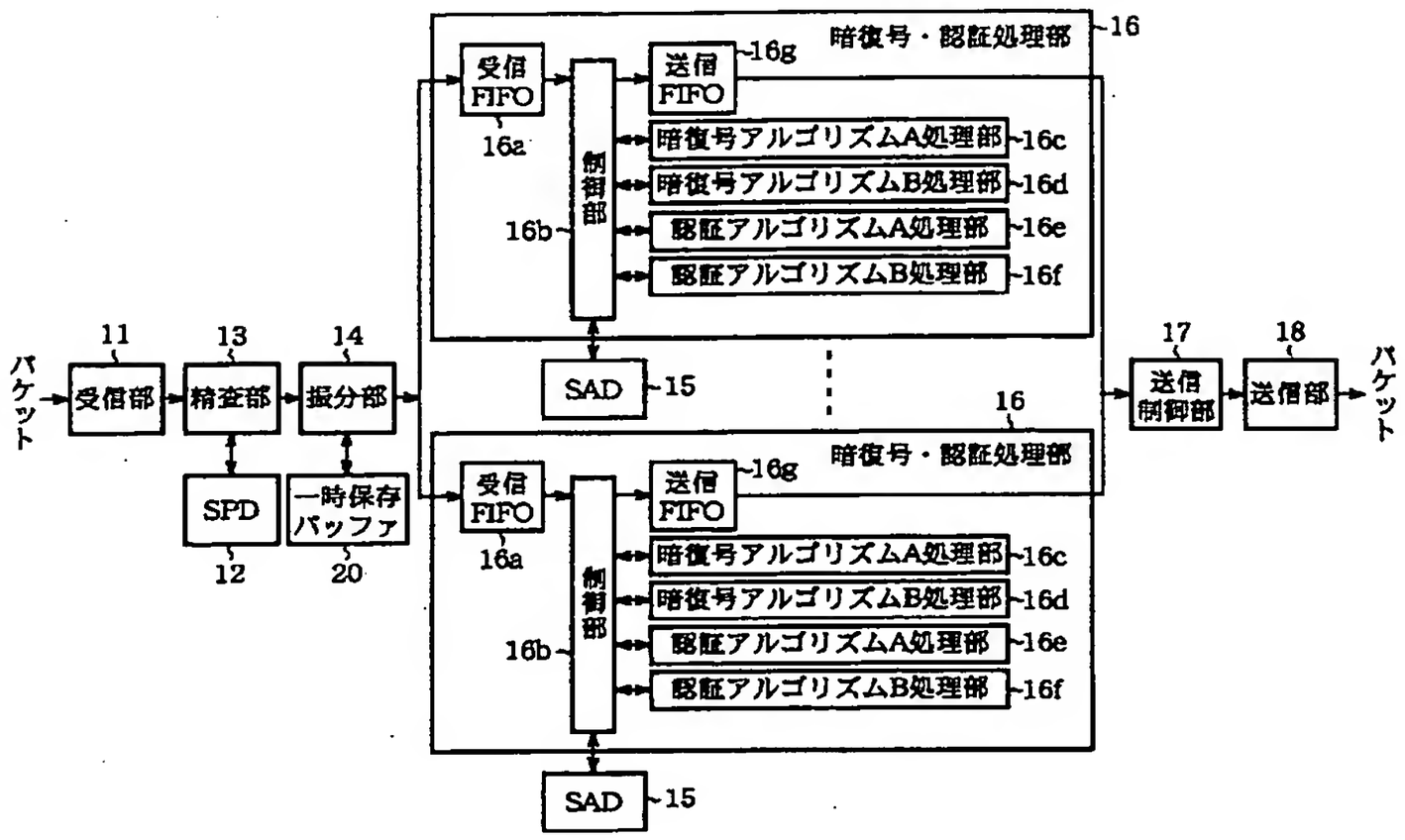
【図４】


スタート
パケットを受信する
ST11
送信先アドレス等をキーにして
SPD内のエントリを検索する
ST12
エントリ内のインデックスを
パケットに付加する
ST13
未処理中の暗復号・認証処理部に
パケットを転送する
ST14
インデックスが指定する
特定エントリから
復号アルゴリズム等を取得する
ST15
認証用のダイジェストを生成する
ST16
ST17
ダイジェストが一致？
NO
YES
ST18
パケットを
廃棄する
パケットの復号化を行う
ST19
処理後のパケットの順序を整列する
ST20
パケットを送信する
ST21
エンド

【図５】


パケット
11
受信部
13
精査部
14
振分部
SPD
12
SAD
更新部
19
SAD
15
16
暗復号・認証処理部
受信
FIFO
16a
制御部
16b
送信
FIFO
16g
暗復号アルゴリズムA処理部
16c
暗復号アルゴリズムB処理部
16d
認証アルゴリズムA処理部
16e
認証アルゴリズムB処理部
16f
17
送信
制御部
18
送信部
パケット

【図６】


パケット
11
受信部
13
精査部
14
振分部
SPD
12
一時保存バッファ
20
暗復号・認証処理部
16
受信FIFO
16a
制御部
16b
送信FIFO
16g
暗復号アルゴリズムA処理部
16c
暗復号アルゴリズムB処理部
16d
認証アルゴリズムA処理部
16e
認証アルゴリズムB処理部
16f
SAD
15
暗復号・認証処理部
16
受信FIFO
16a
制御部
16b
送信FIFO
16g
暗復号アルゴリズムA処理部
16c
暗復号アルゴリズムB処理部
16d
認証アルゴリズムA処理部
16e
認証アルゴリズムB処理部
16f
SAD
15
17
送信制御部
18
送信部
パケット